Mapping of DISA DNS Security Checklist (V4R1.7) Items to NIST 800-81r1 Checklist Items

A Supplement to NIST SP 800-8r1 Secure Domain Name System (DNS) Deployment Guide[1]

Scott Rose
scottr@nist.gov
Date updated: 6/2/2010

Introduction

There are multiple DNS guidance documents available for USG administrators. Besides the NIST Special Publication 800-81r1 Secure Domain Name System (DNS) Deployment Guide, there is a parallel guidance document produced by DISA: The Domain Name System Security Checklist. This checklist is based on the DISA Secure Technical Implementation Guide (STIG) and is included as a prose checklist at the National Checklist Program Repository (found at http://checklists.nist.gov/) and is used by some agencies as the standard configuration and used as a C&A audit checklist.

Below (see Table 1) is a mapping of relevant requirements from the SP 800-81r1 Checklist Items to DISA DNS Security Checklist STIG ID's. This is an attempt to assist administrators who are already following the checklist items in SP 800-81r1 but must conform to the DISA STIG as a C&A audit checklist. Note that the STIG refers to specific versions of BIND and Microsoft Windows Server while the NIST SP 800-81r1 seeks to be more general (but uses BIND and NSD for example configuration snippets) so not all requirements map to checklist items (and vice-versa).

The DISA DNS Security Checklist also includes low level configuration settings for the Operating System (OS) hosting the DNS service. The DISA Checklist also includes operational tasks (like backups and logging) that are best common practice but not fully addressed by NIST SP 800-81r1 checklist items, but are discussed in the guide. For example DISA Checklist item DNS0415 talks about running the DNS server on a dedicated system (with unnecessary services turned off). This is not addressed in a NIST SP 800-81r1 checklist item but is discussed in section 7.2 of the guide. The NIST SP does not go into such low level detail and those requirements will not be included below. This document will only focus on mapping DNS configuration between the two guides.

Special Note on Relevant FISMA Controls: This is not meant to be authoritative for meeting the controls listed. It is simply a guide to help administrators identify which NIST SP 800-81r1 checklist items may help in meeting the FISMA controls listed for a DNS system. There may be other FISMA controls that would apply to the system that are not listed here and some controls listed below may not apply based on the impact level of the system.

Table 1: Comparison of NIST SP 800-81r1 Checklist Items to DISA DNS Security Checklist Items and Possible Related FISMA Controls.

[1] Available at http://csrc.nist.gov/publications/PubsSPs.html

NIST Checklist Item	Related DISA DNS Security Checklist Item	Relevant FISMA Controls (NIST SP 800-53r3)	Notes
1	DNS0130 DNS0402	MA-2	The DISA Checklist item only refers to DISA approved implementations.
2	DNS0130 DNS0140 DNS0190	MA-2 SC-14 SI-5	The DISA Checklist items refer to patch logging, not just keeping the DNS software patched and up to date.
3			
4	DNS0200 DNS0205 DNS0210	CP-7 CP-8 SC-14 SC-22	
5	DNS0160	SC-22	
6	DNS0160 DNS0405 DNS0475 DNS0505 DNS0815	SC-22	DNS0815 refers to MS Windows configuration to disable use of forwarders.
7	DNS0405 DNS0460 DNS0470 DNS0475 DNS0480	SC-14 SC-22	
8	DNS0160 DNS0455 DNS0705 DNS0900	SC-8 SC-12 SC-13 SC-14	DNS0705 says the TSIG secret string must be 160-bits, longer than recommended in the NIST checklist item 8. However, the NIST recommendation calls for 112 bits of security, which means that the actual TSIG string may be longer than 112 bits to insure 112 bits of security (depending on the random number generator in use on the key generation system). DNS0900 refers to the APP session shared secret used by Cisco Content Switch.
9	DNS0450 DNS0455 DNS0250 DNS0720 DNS0810 DNS0915	SC-8 SC-12 SC-13 SC-14	The NIST checklist item is primarily concerned with zone transfer, but later text discusses using TSIG for dynamic update. DNS0915 refers to APP sessions between Cisco Content Switches.
10	DNS0145	AC-2	Note that the BIND dnssec-keygen

	DNS0420 DNS0710	SC-8 SC-12 SC-13	utility generates two files for the TSIG secret string.
11	DNS0145	SC-8 SC-12 SC-13	
12	DNS0145 DNS0455	AC-2 SC-8 SC-13	
13	DNS0145 DNS0420	AC-2 SC-8 SC-13	
14	DNS0145 DNS0455	SC-8 SC-12 SC-13 SC-14	
15	DNS4710	SC-14 SC-20	
16	DNS0420	AC-2 SC-12 SC-13 SC-14 SC-20	
17	DNS4640 DNS4700	SC-14 SC-20	It is assumed in the text of the NIST guide that signed zones will have both a ZSK and KSK.
18		SC-20	
19			
20			
21			
22	DNS0150 DNS0220 DNS0225 DNS0235		The NIST checklist item only refers to RR Types that may have information leakage risks to an enterprise (e.g. HINFO, LOC, RP and TXT).
23	DNS0150 DNS0220 DNS0225 DNS0235		The NIST checklist item only refers to RR Types that may have information leakage risks to an enterprise (e.g. HINFO, LOC, RP and TXT).
24		SC-13 SC-14 SC-20	
25		SC-13 SC-14 SC-20	

26		SC-14 SC-20	
27		SC-14 SC-20	
28	DNS4670 DNS4690	SC-12 SC-13 SC-14 SC-20	
29		SC-12 SC-13 SC-20	
30		SC-12 SC-13 SC-20	
31		SC-12 SC-13 SC-14 SC-20	
32		SC-12 SC-13 SC-14 SC-20	
33		SC-14 SC-20	
34		SC-14 SC-20	